NS Project Phase 1

The Gatekeepers

November 2023

1 Problem Statement:

Owners of startups and small projects often prioritize implementing their servers and focusing on business logic, with system security frequently becoming an afterthought. Those who do consider security typically rely on third-party services such as Cloudflare and AWS WAF, depending on their specific implementation needs. However, accessing additional features on these platforms can be costly, making security maintenance a financial challenge as well.

2 Idea:

Our team is eager to introduce a comprehensive security solution for any server implementation. This solution will operate in tandem with the server instance, filtering packets and performing operations to protect the server from downtime. It will also ban requests from IPs that appear to be malicious actors. Intended as an open-source project, our solution can be configured and utilized according to individual needs. We anticipate that the community will help keep this project thriving as we continue to contribute to our repository, constantly seeking solutions for the latest vulnerabilities.

3 Initiation:

We plan to begin by developing a simple packet sniffer that will intercept all packets directed towards the hosted instance. These packets will then be analyzed by our system. In parallel, a machine learning model will be employed to detect patterns indicative of a DDoS attack. Packets from suspected IPs will be dropped, while requests from valid users will be preserved.

4 References

https://github.com/R3d1001/openflare/blob/main/NSPP1.texLink to the source code